



NCSA IRST Lightning Talks Lunch

Account and Password Hygiene

James Eyrich

Manager NCSA IRST



Account and Password Hygiene

- Random - real random, use a generator
- Long - the max allowed by the site, probably no need for more than 31 at this time.
- No Reuse

Do not let people watch you type a password

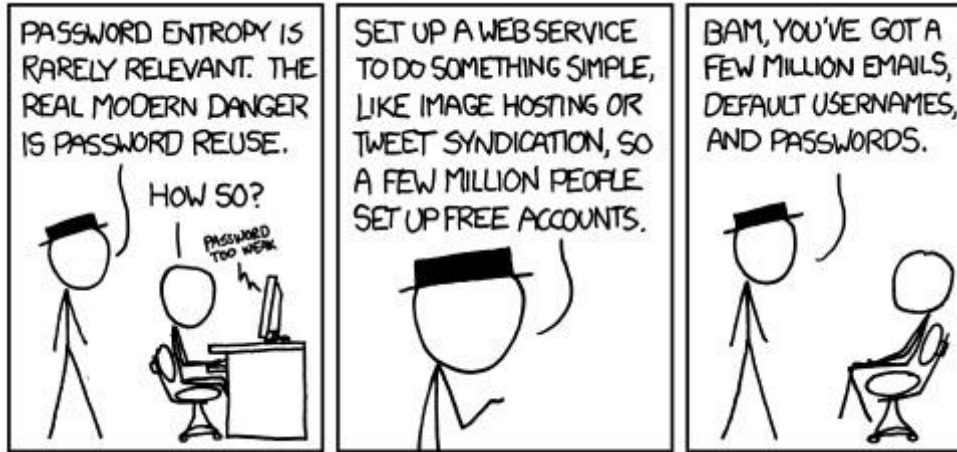
Safe Passwords

- Use different passwords for EVERYTHING
 - Use 14 char or more random passwords
 - Multiple character sets
 - Upper, Lower, Numbers, Symbols
 - The longer the fewer char sets needed

Safe Passwords - Exceptions

- Only use memorable ones for a few important things
 - Campus NetID
 - NCSA Kerberos
 - Desktop/Laptop account
 - Amazon - 😊
 - password manager

Why Not Reuse



- Bad websites
- Hacked websites
- Exposed account details



Password Managers

- Paper
 - Better than reuse.
 - Effective if you generate random passwords
 - Must keep on person, must protect.
 - In general protecting from Internet not a mugger/thief.
- Browser Built-in
 - New features for creating random passwords
 - Better than password reuse
 - Getting better - Sync / Local protection

Cont -

Password Managers Cont

- LastPass
 - Personal - free vs paid, many features now in free
 - Family Accounts
 - 2 factor - some in free, Yubikey requires premium.
 - Allows Sharing to groups
 - Enterprise
 - NCSA Provides this to Staff - help+security@ncsa.illinois.edu
 - Requires Multi Factor Authentication
 - Yubikey or NCSA Duo

Do this at least

Strong, separate passwords for your Email, Bank and mobile phone accounts.



Password Questions?

Vulnerability Scanning & Management

Chris Clausen - Lead Security Engineer

Jacob Frasca - Security Analyst

NCSA IRST



Port Scanning

IRST scans NCSA from scan.security.ncsa.illinois.edu (141.142.148.9) and from off-campus and logs TCP ports.

Allows us to quickly check for potential vulnerabilities

Please do not block access from this host

<https://portal.security.ncsa.illinois.edu/scanme/>



Scan results for 141.142.22.20

Addr	FQDN	Port	Service	Count	First Seen	Last Seen	Count Ext	First Seen Ext	Last Seen Ext
141.142.22.20	nscs-cdc.ncsa.illinois.edu	135	None	4325	May 15, 2018, 8:41 p.m.	Feb. 25, 2020, 7:20 a.m.	None	None	None
141.142.22.20	nscs-cdc.ncsa.illinois.edu	445	None	4334	May 15, 2018, 8:39 p.m.	Feb. 25, 2020, 8:19 a.m.	None	None	None
141.142.22.20	nscs-cdc.ncsa.illinois.edu	623	Intel AMT (vPro)	1200	May 17, 2018, 6:23 a.m.	Feb. 25, 2020, 4:19 a.m.	None	None	None
141.142.22.20	nscs-cdc.ncsa.illinois.edu	2179	None	1188	May 29, 2018, 3:43 p.m.	Feb. 25, 2020, 3:28 a.m.	None	None	None
141.142.22.20	nscs-cdc.ncsa.illinois.edu	3389	RDP	9467	May 15, 2018, 12:11 p.m.	Feb. 25, 2020, 7:42 a.m.	5242	May 17, 2018, 2:37 p.m.	Feb. 25, 2020, 7:42 a.m.
141.142.22.20	nscs-cdc.ncsa.illinois.edu	5040	None	1050	May 22, 2018, 4:21 p.m.	Feb. 25, 2020, 4:53 a.m.	None	None	None
141.142.22.20	nscs-cdc.ncsa.illinois.edu	9053	None	509	May 5, 2019, 7:59 a.m.	Feb. 25, 2020, 4:05 a.m.	None	None	None
141.142.22.20	nscs-cdc.ncsa.illinois.edu	16992	Intel AMT (vPro)	4267	May 15, 2018, 12:24 p.m.	Feb. 25, 2020, 7:46 a.m.	None	None	None
141.142.22.20	nscs-cdc.ncsa.illinois.edu	16994	Intel AMT (vPro)	1201	May 21, 2018, 3:09 a.m.	Feb. 25, 2020, 4:18 a.m.	None	None	None

Scan status: complete Found 8 services

Scan me



SSH Auditor

SSH Auditor also runs from scan.security

Tries various user and passwords against SSH

Alerts when credentials in its database allow login

<https://github.com/ncsa/ssh-auditor>



SSH Auditor (example)

man was able to authenticate to 141.142.22.22
via SSH and tunnel at 2018-07-13 13:22:40

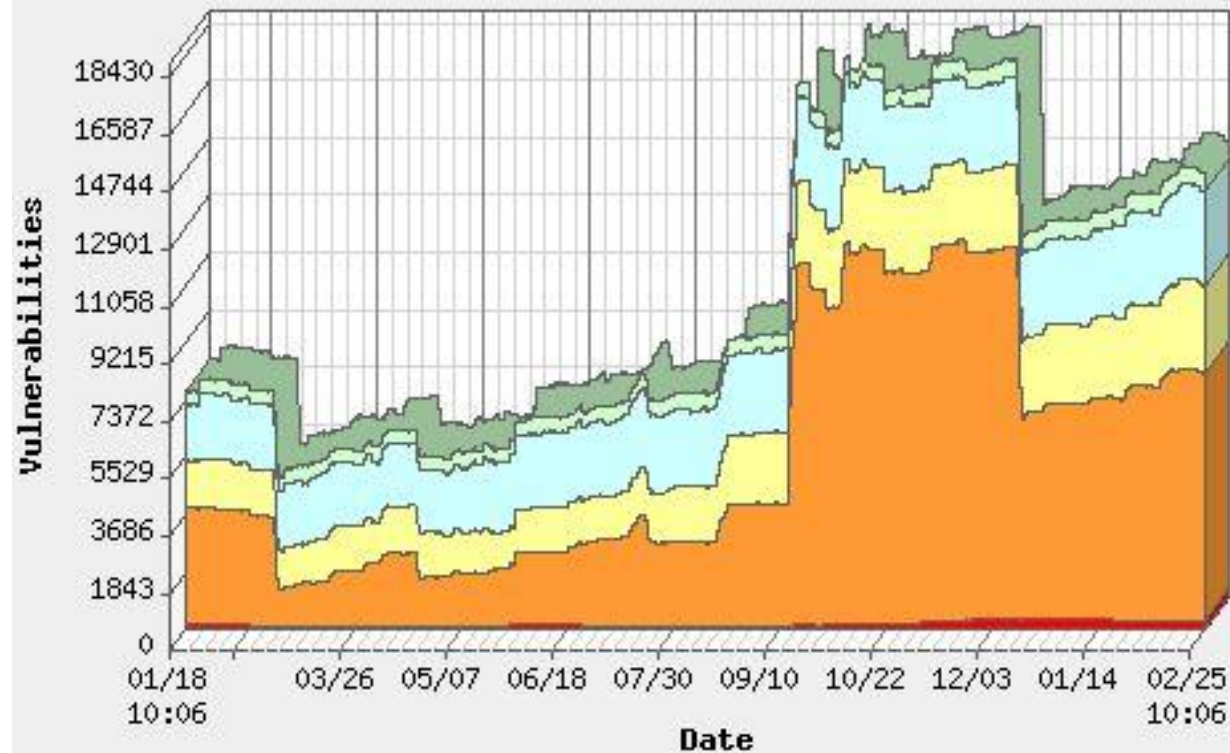
mongodb was able to authenticate to 141.142.22.22
via SSH and exec at 2018-07-13 13:22:40



Qualys scans

Qualysguard is a commercial product that allows IRST to perform vulnerability scans from both the Internet and from on-premises appliances (such as 141.142.148.51)

Qualys tracks scan data that can be used to create reports of potentially vulnerable hosts



Severity Level

266	Severity 5	+142	↑
7933	Severity 4	+4175	↑
2814	Severity 3	+1290	↑
3042	Severity 2	+1249	↑
571	Severity 1	+147	↑
14626 Total		+7003	↑



Scanning/ Vulnerability Management Questions?

Duo Refresher

Kay Avila

Senior Security Engineer

NCSA IRST




What is Duo?

- NCSA's supported two-factor (2FA) / multi-factor (MFA) authentication solution
- Background on what factors are:
 - Something you know - password, PIN
 - Something you have - Duo (phone registration, token, Yubikey)
 - Something you are - biometrics



Multifactor Authentication

LastPass



Please complete multifactor authentication on your phone or mobile device.

No notification? Enter a one-time passcode from your authenticator app.

Authenticate

```
Welcome to the Cerberus Bastion Hosts

Please enter your NCSA Kerberos password, and then accept
the push notification sent to your Duo device.

If you have not setup Duo yet, please do so at:
https://duo.security.ncsa.illinois.edu/
Password:
Duo two-factor login for kayavila


Enter a passcode or select one of the following options:


1. Duo Push to XXX-XXX-2600


Passcode or option (1-1): 1
Success. Logging you in...
```


Verizon 10:15 AM 83%

Login Request
Protected by Duo Security



NCSA
cerberus3.ncsa.illinois.edu



kayavila


141.142.148.18
Champaign, IL, US


10:15:23 AM CST
February 25, 2020

SERVER IP
141.142.148.24


Approve


Deny

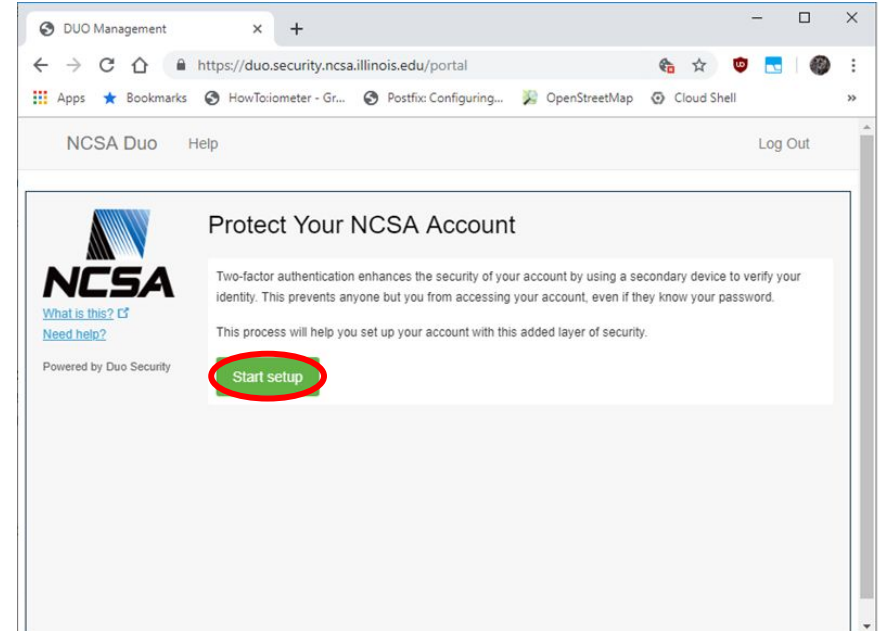
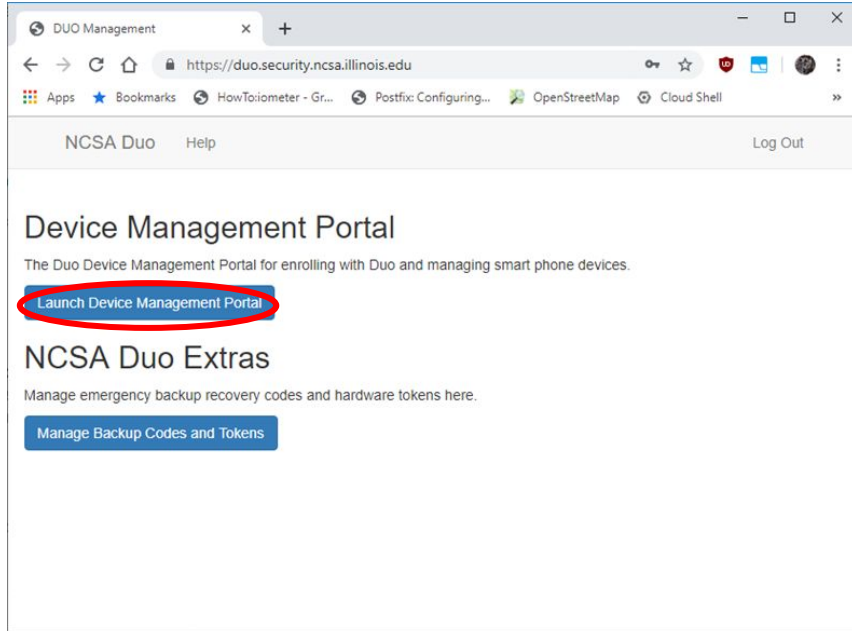


Using Duo

- Visit <https://duo.security.ncsa.illinois.edu> to enroll
- You'll need one of these:
 - Duo app installed on your phone
 - A Yubikey
 - A Duo hardware token

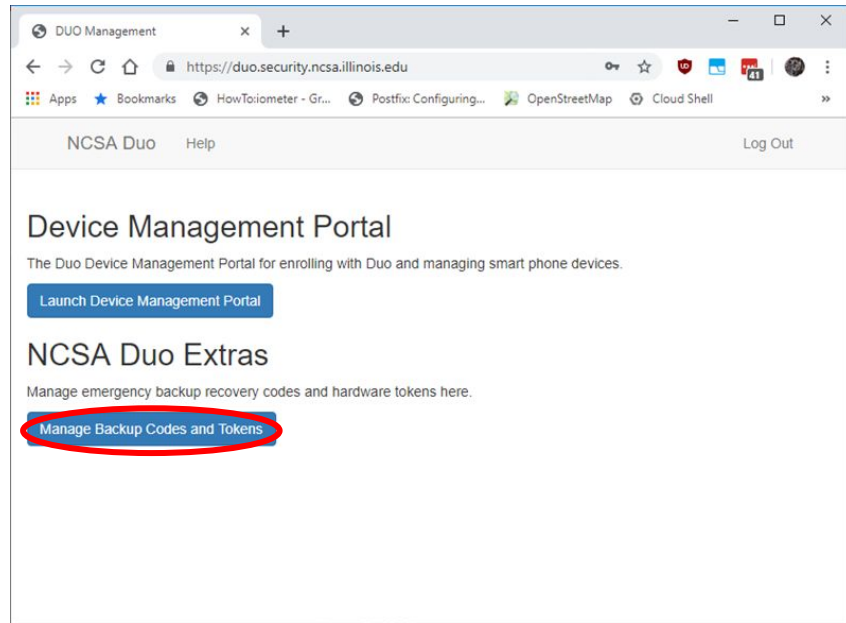


Enrolling



Backup Codes

- One time use “get out of jail free” cards
- **Please set them up!** (Or you’ll get a reminder email every Tuesday...)
- **Store them securely!**



Why can't I use SMS (texts)?

- SMS just isn't secure. (And NIST doesn't recommend it, either.)
 - Texts may pop up even on locked phones
 - SIM cards can easily be transferred between phones
 - SMS messages can be intercepted...

SMS Interception

- Trojans on the device
- “Stingrays” (IMSI catchers) - fake cell phone towers
- Vulnerabilities in the underlying protocol (SS7)
- Someone impersonating you to your provider and making account changes

<https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication/> and
<https://www.dos.ny.gov/consumerprotection/scams/att-sim.html>





Duo Questions?

E-Mail Phishing and Scams

Leandro Avila

Senior Security Engineer

NCSA IRST

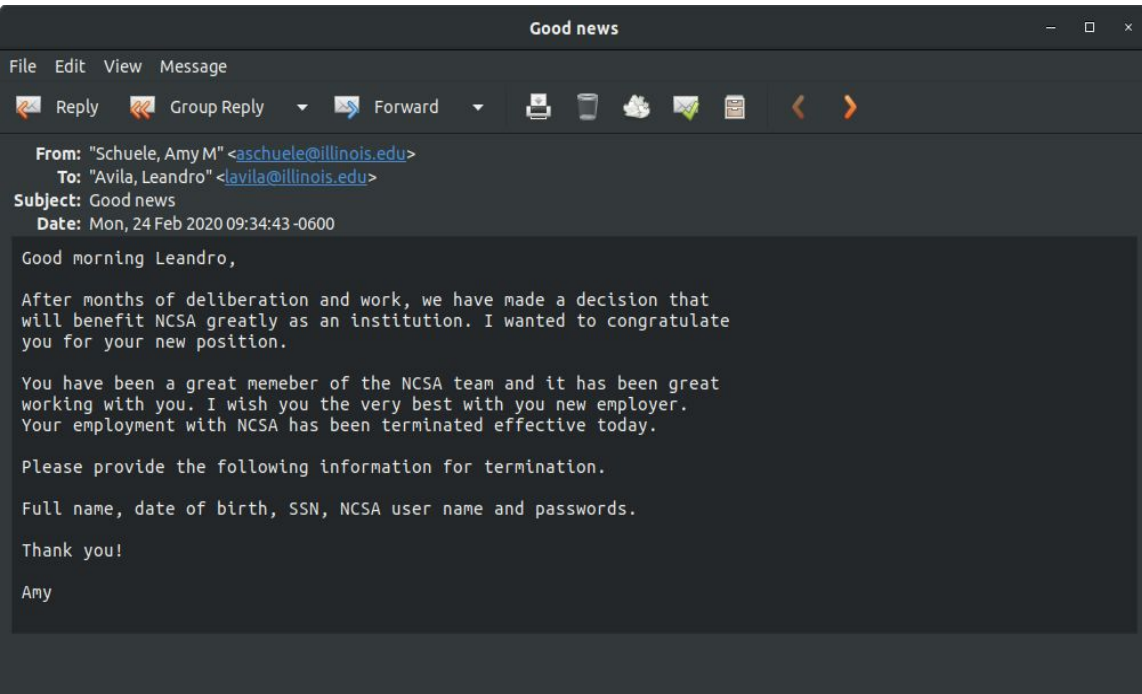


Phishing

- E-mail most common point of entry for malware
- Most clicks shifting to mobile devices
- Be aware of SMS based phishing
- Be always skeptical



Phishing



Always be skeptical.

If in doubt ask IRST

Do not click or reply



Phishing

- Never send private information over email
 - Passwords, SSN, ePHI, Financial
- If you are not expecting the message be suspicious
- Look carefully at the details of the message
 - From address, spelling, etc
- If in doubt call or send a message via Skype/Slack
- <https://techservices.illinois.edu/security/phishing>



Gift Card Scams

You are contacted by someone impersonating your boss/coworker/family/etc. They ask you to buy gift cards and send them the information because they need it quickly

Gift Card Scams

- Gift Cards are like cash
 - If you do not do it with cash, do not do it with gift cards
- Urgency of the request is usually an indicator that something is wrong
- A variation of this will be to wire money



Phishing Questions?

Best Practices Wiki Space

Paul Guder

Senior Security Engineer

NCSA IRST



Purpose of Security Team

- Incident Response
- Hardening & Prevention
- Education, Outreach, & Knowledge Base

Purpose of Security Team

- Security is not just there when things go wrong
- Security is a resource
- There to provide:
 - Configuration Templates
 - Knowledge & Expertise



Best Practices Wiki Space

<https://wiki.ncsa.illinois.edu/display/SecOps/Configuration+Recommendations+and+Best+Practices>

<https://wiki.ncsa.illinois.edu/x/6gjJAQ>



Best Practices Wiki Space

- System Vetting
- Full Disk Encryption
- Service Configuration
 - NTP, openssh, SSSD, Apache, DUO, etc...
- Travel Tips

Security Resources

help+security@ncsa.illinois.edu

<https://wiki.ncsa.illinois.edu/display/SecOps>





Best Practices Wiki Space Questions?